Università degli Studi di Pisa

Facoltà di Ingegneria

Corso di Laurea Specialistica in Ingegneria Informatica

Sviluppo di un sistema di monitoraggio continuo di dati su piattaforma embedded

Relatori:

Prof. Luigi Rizzo

Prof. Marco Avvenuti

Candidato:

Ferdinando Forn a

View metadata, citation and similar papers at core.ac.uk

provided by Electronic Thesis and Dissertation Archive - Università

brought to you by CO

Monitoraggio dei dati

- Tenere traccia, in tempo reale, dei dati transitati o in transito nella rete
- Consentire interrogazioni sul traffico osservato
- Presentare i risultati pianificati in forma diversamente aggregata

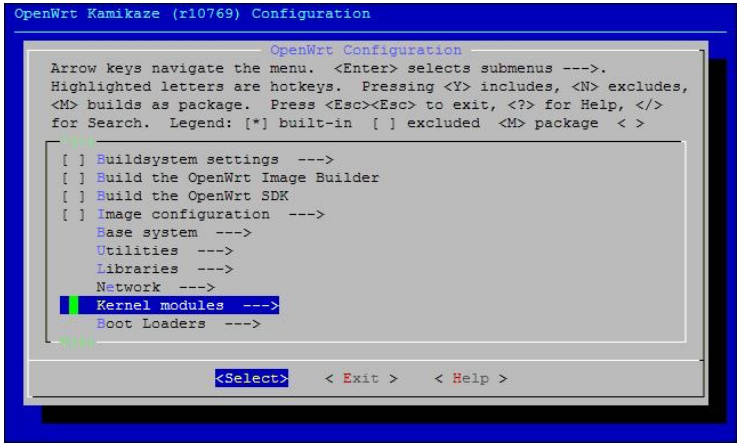
Piattaforma embedded

Realizzando il sistema di monitoraggio su un router, è possibile osservare tutto il traffico che circola nella sottorete.

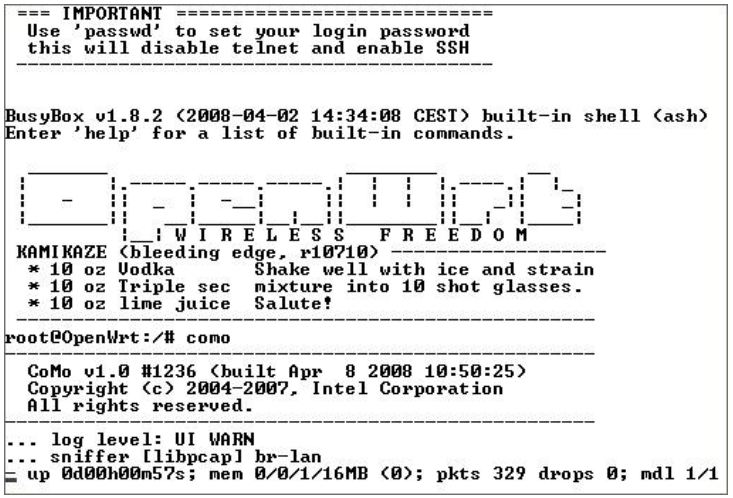
Attraverso le porte USB e seriali del router è possibile aggiungere altre fonti di dati o mezzi di comunicazione.

Il sistema di monitoraggio è realizzato utilizzando software libero, facilmente configurabile e interamente modificabile.

- Distribuzione Linux per sistemi embedded: OpenWRT



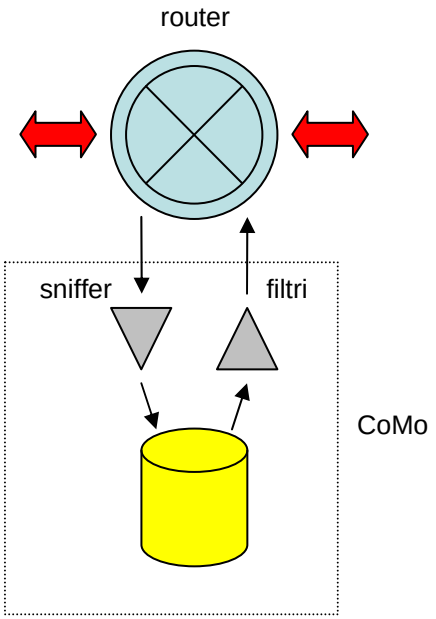
- Applicazione di monitoraggio: CoMo



CoMo è strutturato in un insieme di moduli e un sistema di comunicazione tra di essi e la base di dati.

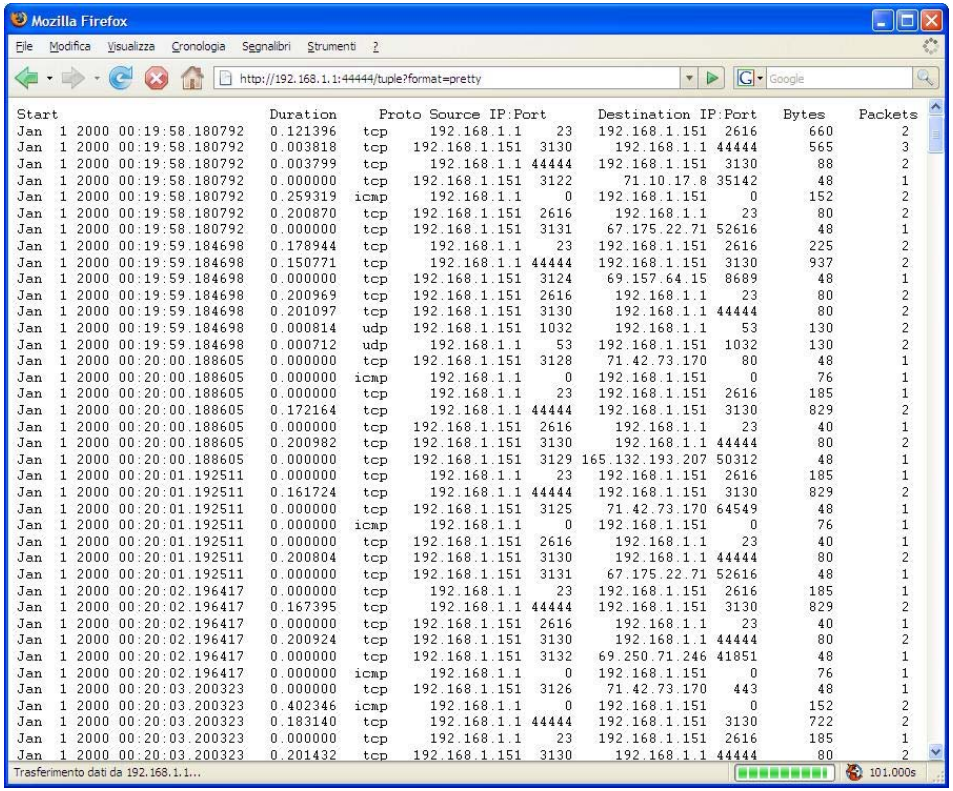
I moduli possono essere:

- Sniffer per la raccolta di dati dalla rete
- Filtri per l'aggregazione e la presentazione dei dati



Accesso ai dati

Le interrogazioni ai filtri possono essere effettuate attraverso una semplice connessione web al router, specificando nell'URL il filtro richiesto e i suoi eventuali parametri.



Start	Duration	Proto	Source IP:Port	Destination IP:Port	Bytes	Packets
Jan 1 2000 00:19:58.180792	0.121396	tcp	192.168.1.1 23	192.168.1.151 2616	660	2
Jan 1 2000 00:19:58.180792	0.003818	tcp	192.168.1.151 3130	192.168.1.1 44444	565	3
Jan 1 2000 00:19:58.180792	0.003799	tcp	192.168.1.1 44444	192.168.1.151 3130	88	2
Jan 1 2000 00:19:58.180792	0.000000	tcp	192.168.1.151 3122	71.10.17.8 35142	48	1
Jan 1 2000 00:19:58.180792	0.259319	icmp	192.168.1.1 0	192.168.1.151 0	152	2
Jan 1 2000 00:19:58.180792	0.200870	tcp	192.168.1.151 2616	192.168.1.1 23	80	2
Jan 1 2000 00:19:58.180792	0.000000	tcp	192.168.1.151 3131	67.175.22.71 52616	48	1
Jan 1 2000 00:19:59.184698	0.178944	tcp	192.168.1.1 23	192.168.1.151 2616	225	2
Jan 1 2000 00:19:59.184698	0.150771	tcp	192.168.1.1 44444	192.168.1.151 3130	937	2
Jan 1 2000 00:19:59.184698	0.000000	tcp	192.168.1.151 3124	69.157.64.15 8689	48	1
Jan 1 2000 00:19:59.184698	0.200969	tcp	192.168.1.151 2616	192.168.1.1 23	80	2
Jan 1 2000 00:19:59.184698	0.201097	tcp	192.168.1.151 3130	192.168.1.1 44444	80	2
Jan 1 2000 00:19:59.184698	0.000814	udp	192.168.1.151 1032	192.168.1.1 53	130	2
Jan 1 2000 00:19:59.184698	0.000712	udp	192.168.1.1 53	192.168.1.151 1032	130	2
Jan 1 2000 00:20:00.188605	0.000000	tcp	192.168.1.151 3128	71.42.73.170 80	48	1
Jan 1 2000 00:20:00.188605	0.000000	icmp	192.168.1.1 0	192.168.1.151 0	76	1
Jan 1 2000 00:20:00.188605	0.000000	tcp	192.168.1.1 23	192.168.1.151 2616	185	1
Jan 1 2000 00:20:00.188605	0.172164	tcp	192.168.1.1 44444	192.168.1.151 3130	829	2
Jan 1 2000 00:20:00.188605	0.000000	tcp	192.168.1.151 2616	192.168.1.1 23	40	1
Jan 1 2000 00:20:00.188605	0.200982	tcp	192.168.1.151 3130	192.168.1.1 44444	80	2
Jan 1 2000 00:20:00.188605	0.000000	tcp	192.168.1.151 3129	165.132.193.207 50312	48	1
Jan 1 2000 00:20:01.192511	0.000000	tcp	192.168.1.1 23	192.168.1.151 2616	185	1
Jan 1 2000 00:20:01.192511	0.161724	tcp	192.168.1.1 44444	192.168.1.151 3130	829	2
Jan 1 2000 00:20:01.192511	0.000000	tcp	192.168.1.151 3125	71.42.73.170 64549	48	1
Jan 1 2000 00:20:01.192511	0.000000	icmp	192.168.1.1 0	192.168.1.151 0	76	1
Jan 1 2000 00:20:01.192511	0.000000	tcp	192.168.1.151 2616	192.168.1.1 23	40	1
Jan 1 2000 00:20:01.192511	0.200804	tcp	192.168.1.151 3130	192.168.1.1 44444	80	2
Jan 1 2000 00:20:01.192511	0.000000	tcp	192.168.1.151 3131	67.175.22.71 52616	48	1
Jan 1 2000 00:20:02.196417	0.000000	tcp	192.168.1.1 23	192.168.1.151 2616	185	1
Jan 1 2000 00:20:02.196417	0.167395	tcp	192.168.1.1 44444	192.168.1.151 3130	829	2
Jan 1 2000 00:20:02.196417	0.000000	tcp	192.168.1.151 2616	192.168.1.1 23	40	1
Jan 1 2000 00:20:02.196417	0.200924	tcp	192.168.1.151 3130	192.168.1.1 44444	80	2
Jan 1 2000 00:20:02.196417	0.000000	tcp	192.168.1.151 3132	69.250.71.246 41851	48	1
Jan 1 2000 00:20:02.196417	0.000000	icmp	192.168.1.1 0	192.168.1.151 0	76	1
Jan 1 2000 00:20:03.200323	0.000000	tcp	192.168.1.151 3126	71.42.73.170 443	48	1
Jan 1 2000 00:20:03.200323	0.402346	icmp	192.168.1.1 0	192.168.1.151 0	152	2
Jan 1 2000 00:20:03.200323	0.183140	tcp	192.168.1.1 44444	192.168.1.151 3130	722	2
Jan 1 2000 00:20:03.200323	0.000000	tcp	192.168.1.1 23	192.168.1.151 2616	185	1
Jan 1 2000 00:20:03.200323	0.201432	tcp	192.168.1.151 3130	192.168.1.1 44444	80	2

Scenario